УДК 003.26

АНАЛІЗ ВЛАСТИВОСТЕЙ ПОДІЛЬНОСТІ ТОДО У МОДИФІКОВАНОМУ ШИФРІ «КАЛИНА»

М. В. Столович[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В данній роботі розглядаються властивості подільності, запропоновані Йосуке Тодо. Ці властивості є узагальненими інтегральними властивостями. Також, розглянуто, яким чином розповсюджуються ці властивості подільності для різних їх представлень. Показано, яким чином розповсюджуються ці властивості при застосуванні до мультимножини відкритих текстів модифікованого шифру «Калина-2», в якому додавання за модулем 2^{64} замінено на додавання за модулем 2.

Ключові слова: властивість подільності, Калина, інтегральний криптоаналіз, SP-мережі

Вступ

Наразі бурхливо розвиваються різні підходи до криптоаналізу симетричних блокових шифрів. Одним із підходів до аналізу шифрів є інтегральний криптоаналіз. Його ідея полягає в розгляданні властивостей відкритих текстів не поодинці, а властивостей їх суми (інтегралу). Однак, наразі цей підхід використовує не усі властивості сум відриктих текстів. Йосуке Тодо в своїй статті[1] запропонував розглядати дещо інші властивості сум відкритих текстів, які виявилися ефективними та застосовними до симетричних блокових шифрів.

1. Попередні позначення

Множини S_k^n та $S_{\mathbf{k}}^{n,m}$

Визначення 1. Нехай множина S_k^n – це підмножина множини F_2^n для будь-якого цілого $k \in \{0, ..., n\}$. Ця підмножина складається з тих елементів $a \in F_2^n$, які задовольняють $k \leq w_a$, де $w_a = \sum_{i=1}^{n} a[i]$.

Тобто,

$$S_k^n \coloneqq \{a \in F_2^n | k \leq w_a\}$$

Визначення 2. Нехай $S_{\mathbf{k}}^{n,m}$ – це підмножина множини $(F_2^n)^m$ для будь-якого вектору $\mathbf{k} \in (\{0, .., n\})^m$. Ця множина складається з тих елементів $\mathbf{a} \in (F_2^n)^m$, які задовольняють $k_i \leq w_{a_i}$, де $w_{a_i} = \sum_{j=1}^{n} a_i[j]$.

Тобто,

$$S_{\mathbf{k}}^{n,m} \coloneqq \{(a_1, a_2, ..., a_m) \in (F_2^n)^m | k_i \leq w_{a_i}, \forall 1 \leq i \leq m\}$$

Функції π_u та $\pi_{\mathbf{u}}$

Нехай $\pi_u : F_2^n \to F_2$ – це функція, яка визначена для будь-якого $u \in F_2^n$. Нехай $x \in F_2^n$ – це аргумент функції π_u. Тоді значення $\pi_u(x)$ – це застосування логічної операція AND для усіх $x[i]$, які задовольняться умові $u[i] = 1$.

Тоді $\pi_u(x)$ рахується як,

$$\pi_u(x) \coloneqq \prod_{i=1}^{n} x[i]^{u[i]}$$

Нехай $\pi_{\mathbf{u}} : (F_2^n)^m \to F_2$ – це функція, яка визначеная для будь-якого $\mathbf{u} \in (F_2^n)^m$. Нехай $\mathbf{x} \in (F_2^n)^m$ – це аргумент $\pi_{\mathbf{u}}$. Тоді $\pi_{\mathbf{u}}(\mathbf{x})$ рахується як

$$\pi_{\mathbf{u}}(\mathbf{x}) \coloneqq \prod_{i=1}^{m} \pi_{u_i}(x_i)$$

Базові поняття інтегрального криптоаналізу

Основна ідея інтегрального криптоаналізу полягає в тому, що ми розглядаємо такі обрані відкриті тексти, для яких сума має інтегральні властивості:

- ALL (A) : Кожне значення присутнє однакову кількість разів в мультимножині.
- BALANCE (B) : Сума усіх текстів мультимножини дорівнює 0
- CONSTANT (C) : Значення слова в усіх відкритих текстах однакове
- UNKNOWN (U) : Множина не має специфічних властивостей, які можна передбачити заздалегіть.

Однак, у інтегральних властивостей є недоліки. А саме:

- невідомо, як розповсюджуються інтегральні властивості, якщо в шифрі присутні небієктивні функції;
- інтегральні властивості не використовують інформацію про алгебраїчну степінь шифру для побудови інтегрального розпізнавача.

Детальний опис інтегрального криптоаналізу наведено у [2].

[a] mstolovych@outlook.com

2. Властивості подільності

Нехай в нас є бієктивна функція, чий алгебраїчний степінь дорінює d. Якщо вхідна мультимножина X має інтегральну властивість A, то вихідна мультимножина теж буде мати властивість A. Якщо ж вхідна мультимножина має властивість B, то вихідна мультимножина буде мати U. Проте, якщо в нас є 2^{d+1} відкритих текстів, то вихідна мультимножина також буде мати властивість B. Класичний інтегральний криптоаналіз не використовує цей факт. А властивості подільності спрямовані на те, щоб використати цю властивість.[1]

Властивість подільності

Визначення 3. Нехай X – це мультимножина, елементи якої приймають значення з F_2^n і k приймає значення між 0 та n. Тоді ми кажемо, що у мультимножини є властивість подільності D_k^n, якщо значення функції π_u завжди парне та w_u менше ніж k. Більше того, парність стає невідомою якщо w_u більше або дорівнює k.

$$\bigoplus_{x \in X} \pi_u(x) = 0, \forall u \in (F_2^n \setminus S_k^n)$$

Розповсюдження властивостей подільності

Нехай s – це булева функція з алгебраїчним степенем d. Якщо вхідна мультимножина аргументів X має властивість подільності D_k^n, то вихідна мультимножина буде мати властивість подільності $D^n_{\lceil k/d \rceil}$.

Більш того, якщо функція s – це перестановка, то вхідна мультимножина зберігає властивість D_n^n.

Векторна властивість подільності

Визначення 4. Нехай X – це множина з елементів множини $(F_2^n)^m$. А $\mathbf{k}$ – це m-мірний вектор, з елементів $0..n$. Мультимножина має векторну властивість подільності, якщо значення функціїї $\pi_{\mathbf{u}}(x)$ для $\forall \mathbf{x} \in X$ завжди парне, якщо $\mathbf{u}$ не належить $S_{\mathbf{k}}^{n,m}$. Більш того парність стає невідомою, якщо $\mathbf{u}$ належить $S_{\mathbf{k}}^{n,m}$.

Розповсюдження векторної властивості

Нехай в нас є S-шар, що складається з множини однакових булевих функцій з алгебраїчним степенем d. Припускаємо, що кожен елемент елементу мультимножини обробляється незалежним чином. Тоді, якщо вхідна мультимножина X мала векторну властивість $D_{\mathbf{k}}^{n,m}$ подільності, то вихідна мультимножина Y буде мати вихідну властивість $D_{\mathbf{k`}}^{n,m}$, де $\mathbf{k`} = \lceil k/d \rceil$.

Колективна властивість подільності

Визначення 5. Нехай X – це мультимножина елементів з $(F_2^n)^m$, та $\mathbf{k}^{(j)}, j \in (1, ..., q)$ – це m-мірні вектори, елементи яких приймають значення $0..n$. Якщо вхідна мультимножина мала властивість $D^{n,m}_{\mathbf{k}^{(1)},\mathbf{k}^{(2)},..\mathbf{k}^{(q)}}$, то значення $\pi_{\mathbf{u}}(x)$ для $\forall \mathbf{x} \in X$ завжди парне, якщо $\mathbf{u}$ не належить об'єднанню $S^{n,m}_{\mathbf{k}^{(1)}} \cup S^{n,m}_{\mathbf{k}^{(2)}} ... \cup S^{n,m}_{\mathbf{k}^{(q)}}$. Більш того, парність стає невідомою, якщо $\mathbf{u}$ належить $S^{n,m}_{\mathbf{k}^{(1)}} \cup S^{n,m}_{\mathbf{k}^{(2)}} ... \cup S^{n,m}_{\mathbf{k}^{(q)}}$.

Розповсюдження колективної властивості

Маючи ті ж самі припущення, що і до векторної властивості подільності. Ми можемо стверджувати, що якщо вхідна мультимножина мала колективну властивість подільності $D^{n,m}_{\mathbf{k}^{(1)},\mathbf{k}^{(2)},..\mathbf{k}^{(q)}}$, то вихідна мультимножина буде мати $D^{n,m}_{\mathbf{k`}^{(1)},\mathbf{k`}^{(2)},..\mathbf{k`}^{(q)}}$, де $k`^{(j)} = \lceil k_i^{(j)}/d \rceil$. Більш того, якщо булева функція – це бієкція та $k_i^{(j)} = n$ то, $k`^{(j)}_i = n$ також.

3. Шифр «Калина-2»

Шифр «Калина-2» є державним стандартом України блочного шифрування побудованний на принципі SP-мережі. «Калина-2» є AES-подібним шифром із подібною структурою та раундовою функцією.

Операції зашифрування

Зашифрування відбувається у такі кроки:

1) додавання ключа за модулем 2^{64};
2) раундове перетворення;
   - шар нелінійного відображення;
   - перестановка елементів;
   - лінійне перетворення;
   - функція додавання раундового ключа за модулем 2;
3) останній раунд шифрування має додавання раундового ключа за модулем 2^{64}

Детальний опис шифру «Калина» наведено у[3].

В данній роботі буде розглянуто модифікований варіант шифру «Калина-128/128», де на початку та в кінці додавання йде додавання не за модулем 2^{64}, а за модулем 2.

4. Застосування властивостей подільності до модифікації шифру «Калина-2»

Нехай, в нас є мультимножина X яка має властивість подільності $D^{n,m}_{\mathbf{k}^{(1)},\mathbf{k}^{(2)},..\mathbf{k}^{(q)}}$, тобто мультимножина i-их координат векторів задовольняє властивості $D^8_{k^{(i)}}$.

Після першого додавання раундового ключа за модулем 2 властивість подільності не зміниться через те, що додавання за модулем два ніяким чином не вплине на значення функції $\pi_u(x)$.

Розглянемо дію раундової функції шифру «Калина-2»:

1) **Байтова підстановка**
   Для шифру «Калина» визначені байтові підстановки. Відомо, що кожна з запропонованих підстановок має алгебраїчну степінь 7. Тому після них, властивість подільності $D^{n,m}_{\mathbf{k}^{(1)},\mathbf{k}^{(2)},..\mathbf{k}^{(q)}}$ перейде у властивість подільності $D^{n,m}_{\mathbf{k`}^{(1)},\mathbf{k`}^{(2)},..\mathbf{k`}^{(q)}}$, де $k' = \lceil k/7 \rceil$
2) **Перестановка елементів**
   Так як властивість подільності кожної байту не залежить від її місцезнаходження при матричному поданні, то після цієї операції властивість подільності збережеться.
3) **Перехід до лінійного перетворення**
   Наразі ми маємо колективну властивість подільності визначену по кожному байту поточного стану шифрування. Проте, функція лінійного перетворення обробляє частини стану по колонкам, а не по байтам. Тому ми повинні визначити

перехід від колективної властивості подільності по байтах до стовпчикових.

Будемо робити це досить прямолінійно. Із-за того, що байт має властивість подільності D_k^n можна сказати, що в нього k бітів мають інтегральний стан A. Спираючись на цей факт, колективна властивість подільності $D^{n,m}_{\mathbf{k}^{(1)},\mathbf{k}^{(2)},..\mathbf{k}^{(q)}}$ переходить у D_q^{8*m}, де $q = \sum_{i=1}^{m} k^{(i)}$, та m – це кількість байтів стану.

4) **Лінійне перетворення**

Лінійне перетворення має алгебраїний степінь щонайбільше 1. Саме цьому використовуючи твердження про розповсюдження властивості подільності[1] маємо, що властивість подільності не зміниться при переході через лінійне перетворення.

5) **Додавання з раундовим ключем**

Як і було розглянуто раніше, додавання з ключем за модулем 2 не змінює значення властивості подільності мультимножини обраних відкритих текстів.

6) **Перехід від шару лінійного перетворення до *S*-шару**

На вході S-шару ми повинні мати колективу властивість подільності, бо ми маємо не один $S-box$, і нам потрібно розбити загальну властивість подільності на колективну.

Перед нами постає задача розбиття D_q^{8*m} на $D^{n,m}_{\mathbf{k}^{(1)},\mathbf{k}^{(2)},..\mathbf{k}^{(q)}}$, де q – це кількість усіх можливих векторів, які задовольняють умові $k^{`(j)}_1 + k^{`(j)}_2 + ... + k^{`(j)}_m = k (1 \le j \le q)$. Ми так робимо, бо ми знаємо сумарну кількість бітів, проте їх розбиття на байти нам невідомо. Тому ми розглядаємо усі можливі варіанти.

Очевидно, що розгляд усіх можливих варіантів розбиття числа k на доданки є досить складною обчислюванною задачею. Саме тому ми застосуємо деяку хитрість щодо цього етапу:

ми вже знаємо, що порядок по-байтових властивостй подільності у колективній властивості подільності не має ніякого значення, бо усі байти «рівноправні». Саме тому нам не потрібно розглядати усі можливі розбиття, а тільки впорядковані набори (відсортовані). Ця хитрість суттєво зменшує обчислювальну складність.

Результати для шифру «Калина-2»

Підготовлюємо відкриті тексти таким чином, що в байті буде властивість D_k^n, якщо k бітів з n будуть пробігати усі можливі значення як k-мірні вектора, а інші $n-k$ бітів будуть константними.

Розглянемо 3-раундовий модифікований шифр «Калина 128/128», де будь-які 7 байтів є активими, а інші константними. Для перших 7-ми байтів будемо мати D_8^8, а для інших – D_0^8 Після першого раунду шифрування кількість активних одночасно бітів зменшиться до 8. Після другого раунду шифрування їх вже буде 1, або один байт буде мати D_1^n, в той час, поки в інших буде D_0^8 Після третього раунду одночасно активних бітів вже не буде, а тому ми можемо будувати атаку за допомогою інтегрального розпізнавача. Загальна кількість текстів, котрі нам потрібні, щоб побудувати множину з такими властивостями подільності дорівнює 2^{56}.

Висновки

В цій статті були розглянуті властивості подільності та розповсюдження цих властивостей при переході через функції з відомою алгебраїним ступенем. Також розглянуто розповсюдження цих властивостей для 3-раундового модифікованного шифру «Калина-2».

Було вираховано скільки потрібно відкритих текстів, задля того, щоб побудувати інтегральний розпізнавач. Властивості подільності використовують алгебраїчний ступень функції, яку застосовують до мультимножини обраних відкритих текстів. Завдяки цьому властивості зберігаються в більшій кількості раундів аніж в інтегральному криптоаналізі. Слід також зазначити, що кількість необхідних текстів та обчислювальна складність зростаються експоненційно.

Перелік використаних джерел

1. Todo Yosuke. Structural Evaluation by Generalized Integral Property. — Cryptology ePrint Archive, Report 2015/090. — 2015. — `http://eprint.iacr.org/2015/090`.
2. Knudsen Lars, Wagner David. Integral cryptanalysis // International Workshop on Fast Software Encryption / Springer. — 2002. — P. 112–127.
3. Oliynykov Roman, Gorbenko Ivan, Kazymyrov Oleksandr et al. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. — Cryptology ePrint Archive, Report 2015/650. — 2015. — `http://eprint.iacr.org/2015/650`.